

УДК 519.688; 681.3, 519.7

НОВАЯ МОДЕЛЬ ВЫЧИСЛЕНИЙ – КГТ-2¹

П.А. Правильщиков

Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: pavelp@ipu.ru

Т.М. Васильева

Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: tvassa@mail.ru

Ключевые слова: квантовые компьютеры, квантовые ускорители, механизм квантового параллелизма, новые модели вычислений, квантовые алгоритмы, квантовый регистр, куниты, куэнки.

Аннотация. Приведена схема новой модели вычислений для модульных проблемно-ориентированных квантовых компьютеров (КК) в виде квантового генератора тестов-2 (КГТ-2), где используется механизм параллелизма, подогнанный под выполнение квантовых D-алгоритмов (QD-алгоритмов). Показано, что сегодня для создания надежных КК их регистр должен быть построен на сложных кунитах - см. [2]). Вводится термин «куэнк» для обозначения сложного кунита, содержащего небольшое число λ запутанных кубитов ($2 \leq \lambda \leq 50$). Продемонстрировано, что модульные КК и их модель в виде КГТ-2 преодолевают проблемы с использованием большого числа L ($L > 50$) запутанных кубитов при разработке КК (см. [1]), а при решении NP-полных задач на платформе КГТ-2 временная сложность является полиномиальной [3, 4].

1. Схема новой модели вычислений

В ИПУ РАН теоретически обоснован и разрабатывается проблемно-ориентированный КК, т.е. квантовый ускоритель (КвУ). В [1] приведены основы новой модели вычислений для КвУ. В данном докладе приведена схема КГТ-2 и ее описание. Но прежде подчеркнем, что всякий КК управляется классическим компьютером с помощью лазерных, СВЧ или других импульсов (см. рис. 1). Это показано в модели идеального КК в [5] (см. также [6, 7]). Подчеркнем, что в [5], регистр КК построен на кубитах.

Здесь можно упомянуть о критериях ди Винченцо [8]. Их можно называть постулатами квантового компьютеростроения. Так, необходим процесс инициализации разрядов (т.е. кунитов) в регистре КК. Напомним, что кунитом (англ. эквивалент *qudit*) называют квантовый разряд в регистре, физической основой которого служит квантовая система (например, ядро атома), имеющая ν состояний. Если каждому состоянию системы, которое определяются, например, спином атомного ядра, сопоставить некоторое число, то с учетом *принципа суперпозиции* в квантовой механике (КМ) кунит может одновременно содержать ν чисел. Обозначим кунит в регистре QR символом k_ℓ ($\ell = \overline{1, L}$).

¹ Данный доклад, по сути, является продолжением доклада *Правильщиков П.А.* «Закат кремниевых технологий и квантовая революция в вычислительной технике» здесь же на ВСПУ-2019 – см. Труды ВСПУ-2019 [1]. Здесь сохранены: нумерация формул и аббревиатуры, а также обозначения, принятые в [1].

Тогда $v = \dim H_\ell$ – см. [1] и состояние квантовой системы описывается суперпозицией – см. выражения (2)-(5) в [1].



Рис. 1. Схема соединения КК и управляющего им классического компьютера.

Теоретически число $v > \tilde{N}$, где \tilde{N} – любое наперед заданное число \tilde{N} . В настоящее время, как утверждает американский физик Д. Авшалом, практически достижимым, считается число $v \approx 10^7$. Это число будет достигаться постепенно: сначала будут освоены КК, у которых регистр содержит кубиты, затем – регистры с кутритами, а затем с куквадритами и т.д. Необходимо также иметь аппаратуру для измерения состояния регистра, содержащего результат, полученный в качестве решения задачи. Процессор КК или КвУ должен выполнять некоторый универсальный (базисный) набор унитарных преобразований, реализуемых квантовыми логическими элементами (вентильями). Система, реализующая регистр КвУ, должна содержать достаточно большое число разрядов, управляемых СВЧ, электромагнитными или лазерными импульсами в процессе выполнения соответствующих операций – см. рис. 1. Следует обеспечить за время Δt_d – время до декогерентизации – выполнение требуемой совокупности логических операций, в частности, операций пересечения кубов. По сути, операции пересечения кубов реализуют операцию $A \setminus B$, т.е. в результате будет получена «разность множеств $A \setminus B$ » – см. [9]. Управляющие импульсы должны контролироваться с точностью не хуже 10^{-4} .

К постулатам ди Винченцо добавим постулаты, которые необходимы для реализации нашего КвУ, вычислительной моделью которого является КГТ-2. Заметим, что КвУ ориентирован на решение булевых и алгебраических уравнений [4, 10] и, в частности, на решение некоторых NP-полных задач (например, SAT-задачи [4]).

Постулат 1. Для решения обратной задачи \tilde{I} для булевых уравнений (т.е. SAT-задачи) достаточно найти или построить хотя бы один вектор X_i – см. [11].

Постулат 2. В результате измерения кунита всегда будет получено только одно число из v чисел, содержащихся в этом куните, с вероятностью $|a_{\xi}|^2$ – см. (2) в [1].

Для решения SAT-задачи в соответствии с постулатом 1 необходим только один вектор X_i из n переменных [11]. Например, вектор $X_i = \langle 0111 \rangle$ для $n = 4$, где n – число аргументов в булевом уравнении. Для этого придется использовать n кунитов, которые при измерении дадут по одному значению вектора X_i в каждом куните, но в результате будет получено n значений вектора X_i переменных. Так, например, для $X_i = \langle 0111 \rangle$ понадобится 4 кунита. Из каждого кунита при подготовке к измерению, используя вспомогательные квантовые схемы, можно получить только одно нужное нам значение вектора X_i . См. [12, 13].

Постулат 3. Сумма квадратов модулей амплитуд суперпозиции для каждого кунита равна единице. Таково условие нормировки – см. выражение (2) в [1].

Постулат 4. Несмотря на то, что в L разрядах (кунитах) может храниться v^L чисел, в соответствии с принципами КМ в процессе измерения («квантового считывания») можно получить только одно L -разрядное число (см. также постулат 2). Здесь L – длина регистра КК (т.е. L – число квантовых разрядов в регистре).

Постулат 10. Любая унитарная матрица U^\dagger описывает физически возможный квантовый вентиль – см. [14, стр. 40]. Другими словами: матрица U_k^\dagger , описывающая квантовый элемент φ_k (т.е. квантовый вентиль φ_k), должна быть унитарной: $U_k = U_k^\dagger$. Частным случаем унитарной матрицы U^\dagger является *ортогональная матрица*. Эволюция *замкнутой* квантовой системы описывается *унитарным преобразованием* (матрицей U^\dagger), т.е. постулат 10 является следствием постулата об эволюции квантовой системы – см. [14, 15]. Если начальное состояние системы определяется вектором $|\psi_0\rangle$, то после завершения эволюции оно будет: $|\psi_1\rangle = U^\dagger(|\psi_0\rangle)$.

Одной из двух моделей КвУ служит схема квантового генератора тестов (КГТ-1). КГТ-1 содержит два регистра построенных из *простых* кунитов. Его схема приведена в [6, 7]. Здесь приведена схема другой модели в виде КГТ-2 (рис. 2). В КГТ-2 имеются регистры QR_1 и QR_2 , построенные из куэнков $q_{1,\ell}$ [2]. Число L куэнков в QR_1 и QR_2 одинаково ($\ell = \overline{1, L}$). Предполагается, что куэнк $\alpha_{1,\ell,i}$ в QR_1 или куэнк $\alpha_{2,\ell,i}$ в регистре QR_2 содержат одинаковое число λ *запутанных* кубитов ($2 \leq \lambda \leq 50$) и i изменяется от 2 до λ . На рис. 2 представлен простейший случай, когда $\lambda = 2$. Классический компьютер, управляющий КГТ-2, на рис. 2 не показан (см. рис. 1). Блок настройки и коммутации «помогает» классическому компьютеру управлять в целях реализации операций с использованием квантовых вентилях, в частности, операций, реализуемыми квантовыми блоками пересечения QB_ℓ над разными куэнками [16,17]. Описание схем фильтрации и пролиферации при использовании QD-алгоритмов приведены в [3,4,16]. Регистр QR_1 на рис. 2 изображен дважды, так как результат вычислений помещен в QR_1 . После измерения, квантовая информация, содержащаяся в QR_1 , превращается в классическую [14, 15].

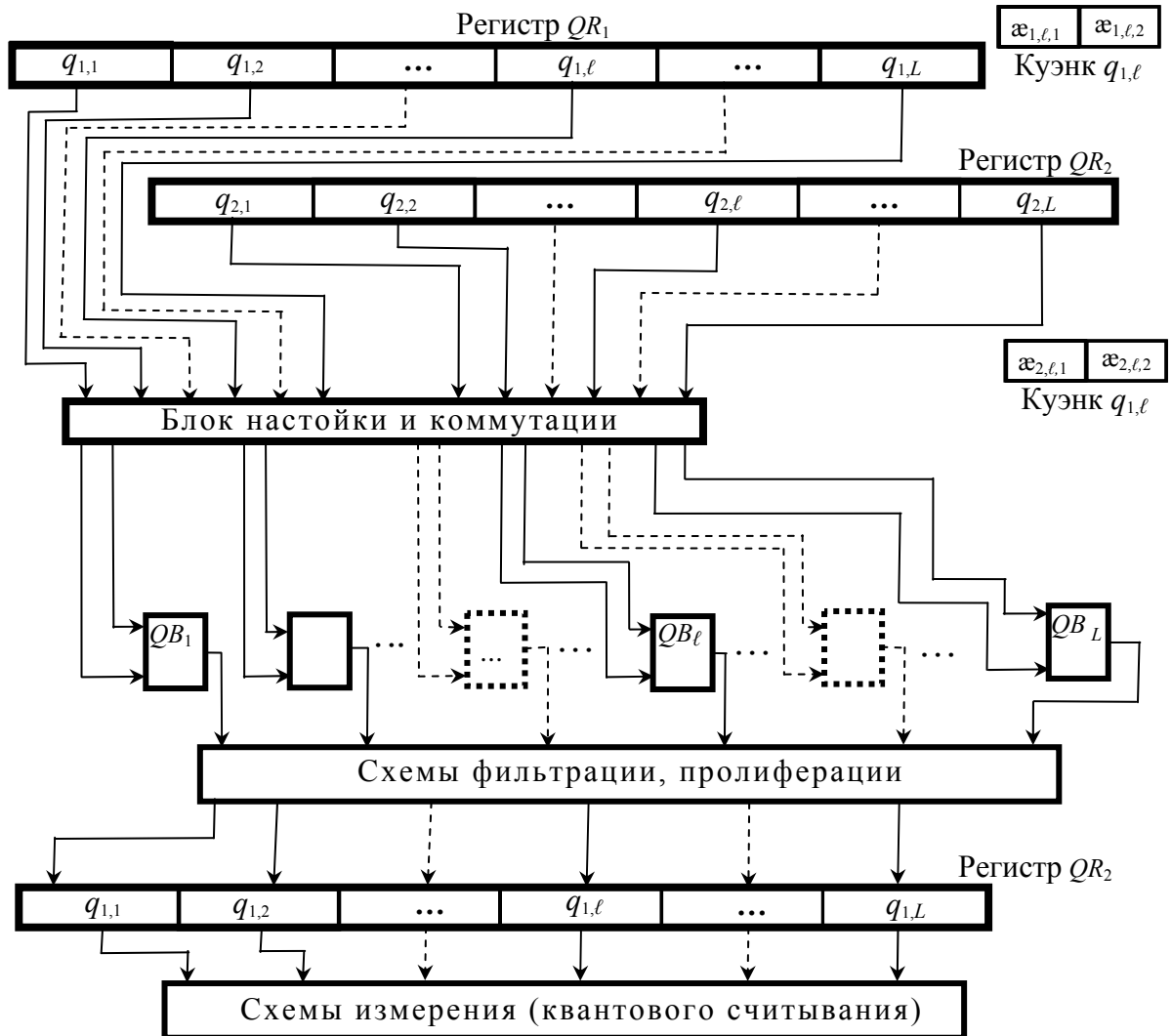


Рис. 2. Вычислительная модель КВУ в виде схемы КГТ-2.

Покажем, как куэнк связан с простым кунитом, а точнее с частным случае такого кунита – куквадритом. Для этого в простейшем случае, когда $\lambda = 2$, запишем вектор состояния – вектор $|\psi\rangle_{v=4}$ куэнка:

$$(1) \quad |\psi\rangle_{v=4} = a_1|00\rangle + a_2|01\rangle + a_3|10\rangle + a_4|11\rangle \quad |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 = 1.$$

Здесь предполагается, что для решения многих задач с помощью нашего КВУ (например, для решения булевых уравнений [4]) амплитуды являются действительными числами. В этом случае конечное векторное пространство, которое используется для описания квантового разряда или всего квантового регистра, в линейной алгебре называют *евклидовым* [18, с. 426]. Однако в теории квантовых вычислений в соответствии с традициями КМ для описания квантового разряда или регистра КК используется термин «*гильбертово пространство*», обозначаемое символом H - см. [1]. Теперь в (1) переобозначим двоичные числа в дираковских скобках на десятичные числа: $|00\rangle \rightarrow |0\rangle$, $|01\rangle \rightarrow |1\rangle$, $|10\rangle \rightarrow |2\rangle$, $|11\rangle \rightarrow |3\rangle$. Тогда получим ту же суперпозицию вектора $|\psi\rangle_{v=4}$ для куэнка в другой форме:

$$(2) \quad |\psi\rangle_{v=4} = a_1|0\rangle + a_2|1\rangle + a_3|2\rangle + a_4|3\rangle \quad |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 = 1.$$

Выражение (2) полностью совпадает с выражением (5) для куквадрита в [1]. Это говорит о том, что математический аппарат, созданный для простых кунитов, может быть использован и для описания унитарных операций с куэнками в регистре модульного КК [19]. В схеме КГТ-2 рис. 2 регистры QR_1 и QR_2 построены из куэнков. Куэнк $q_{1,\ell}$ из QR_1 и куэнк $q_{2,\ell}$ из QR_2 построены из 2-х запутанных кубитов: $\mathfrak{x}_{1,\ell,1}$ и $\mathfrak{x}_{1,\ell,2}$. На рис. 2 куэнк $q_{1,\ell}$ является первым входом блока QB_ℓ . Вторым входом является куэнк $q_{2,\ell}$.

Следует повторить, что сегодня практически достижимым для простых кунитов является число $v \approx 10^7$, тогда как для куэнка с $\lambda = 50$ основываясь на опыте ИВМ, практически достижимым является число $v = 2^{50} \approx 1,12 \cdot 10^{15}$. Теперь сравним два регистра QR_a и QR_b , у которых $L_a = L_b$. Регистр QR_a построен из простых кунитов $k_{1,\ell}$, а QR_b – из куэнков $q_{b,\ell}$ ($\lambda \geq 2$). Предположим, что для кунита $k_{a,\ell}$ и куэнка $q_{b,\ell}$ размерность v одинакова и при этом $v > 2$. Пусть реальный физический объем кунита $q_{b,\ell}$ из QR_a равен реальному объему кубита $\mathfrak{x}_{b,\ell,c}$, входящего в куэнк $q_{b,\ell}$. Известно, что в «*гильбертовом пространстве много места*» [10]. Следовательно, реальный физический объем V_a регистра QR_a всегда меньше, чем реальный физический объем V_b регистра QR_b : $V_a < V_b$. В этом свойстве регистра QR_a , построенного из простых кунитов, состоит главное преимущество их использования: при одном и том же числе L , чем больше размерность v гильбертова пространства кунита $k_{a,\ell}$, тем меньше его реальный физический объем V_a .

2. Заключение

В наши дни существует «*крошечное меньшинство*» скептиков, считающих, что КК не появятся в «*обозримом будущем*», а «*большие*» КК, у которых регистр содержит 1000 кубитов не появятся никогда [19]. Напомним, что история ВТ хранит высказывания подобных скептиков, о классических компьютерах еще со времен появления первого ЭНИАКа (ENIAC, сокр. от *Electronic Numerical Integrator and Computer*). Эти высказывания были опровергнуты эволюцией компьютеров в соответствии с законом Мура. Напротив, те, кто реально занимается разработкой КК и уже разработали КК, утверждают, что «*Пришло время перестать задавать вопрос, возможен ли КК, и начать фокусировать деятельность на разработке его крупномасштабной архитектуры и на том, что он способен делать*» [20]. Сегодня они пытаются создать *модульный* КК, так как подход, основанный на «*грубой силе*», т.е. на постоянном добавление запутанных кубитов к регистру КК, по их мнению, обречен на неудачу – см. также [1].

Список литературы

1. Правильщиков П.А. Закат кремниевых технологий и квантовая революция в вычислительной технике // Труды XIII Всероссийского совещания по проблемам управления ВСПУ-2019. Москва, 17-20 июня 2019 г. М.: Институт проблем управления им. В.А. Трапезникова РАН, 2019.
2. Правильщиков П.А. Простые и сложные (составные) куниты в регистре квантового компьютера / Пленарный доклад // Труды 18-ой Международной молодежной конференции «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта» CAD/CAM/PDM-2018. М.: Институт проблем управления РАН им. В.А. Трапезникова РАН, 2018. С. 17.
3. Правильщиков П.А. Закон сохранения перебора и естественный параллелизм **D**-алгоритмов для построения тестов и моделирования в технической диагностике. // Автоматика и телемеханика. 2004. № 7. С. 156-199.

4. Правильщиков П.А. Квантовое решение булевых уравнений и проблема $P = ? NP$ // Информационные технологии в проектировании и производстве. 2018. № 1. С. 50-64.
5. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежды и реальность. Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2002. 320 с.
6. Правильщиков П.А. Квантовый параллелизм и новая модель вычислений // Труды XII Всероссийского совещания по проблемам управления ВСПУ-2014. Москва, 16-19 июня 2014 г. М.: Институт проблем управления им. Трапезникова РАН. 2014. С. 7319-7334. ISBN 978-5-91450-151-5.
7. Правильщиков П.А. Новый механизм квантового параллелизма и его физические и математические основания // Информационные технологии в проектировании и производстве. 2017. № 4. С. 15-26.
8. DiVincenzo D.P. The physical implementation of quantum computation // Forthscr. Der Phis. 2000. В. 48. No. 9-11. P. 771-783.
9. Правильщиков П.А. Теоретико-множественные основания новой модели вычислений – КГТ // Информационные технологии в проектировании и производстве. 2017. № 3. С. 20-28.
10. Правильщиков П.А. Квантовое превосходство и решение алгебраических уравнений // Информационные технологии в проектировании и производстве. 2018. № 3. С. 49-60.
11. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. 584 с.
12. Правильщиков П.А. Решение проблемы подготовки к измерению кунитов в регистре квантового компьютера // Труды 16-й международной конференции «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта» (CAD/CAM/PDM-2016). М.: Институт проблем управления РАН им. В.А. Трапезникова РАН, 2015. С. 78-82. ISBN 978-5-905675-71-3.
13. Правильщиков П.А. О решении проблемы подготовки к измерению кунитов в регистре квантового компьютера // Информационные технологии в проектировании и производстве». 2016. № 3. С. 34-41.
14. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация / Пер. с англ. М.: Мир, 2006. 824 с.
15. Прескилл Дж. Квантовая информация и квантовые вычисления. Москва-Ижевск: ИКИ (НИЦ Регулярная и хаотическая динамика), 2008. 464 с. (см. стр. 30).
16. Правильщиков П.А. Новая квантовая математика: матричное исчисление кубических комплексов и квантовые D-алгоритмы. // Информационные технологии в проектировании и производстве. 2017. № 2. С. 21-32.
17. Правильщиков П.А. Простые и сложные (составные) куниты в регистре квантового компьютера / Пленарный доклад // Труды 18-ой Международной молодежной конференции «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта» (CAD/CAM/PDM-2018). М.: Институт проблем управления им. В.А. Трапезникова РАН. 2018. С. 19-23. ISBN 978-5-91450-226-0.
18. Бортаковский А.С., Пантелеев А.В. Линейная алгебра в примерах и задачах. М.: Высшая школа, 2010. 591 с.
19. Dyakonov M. The Case Against Quantum Computing // IEEE Spectrum. 2018 (15 Nov). Электронный ресурс 24.11.2018: URL: <https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing>
20. Лукин М., Монро К., Шелькопф Р. Квантовые связи // В мире науки. 2016. Июль. Электронный ресурс 1.10.2018: URL: <http://scientifically.info/news/2016-08-10-3251>